Call for Papers: DIMVA 2020

17th International Conference on
Detection of Intrusions and Malware & Vulnerability Assessment

Lisbon, Portugal - June 24-26, 2020

The CFP is available in PDF format here.

Important Dates:

Paper Submission Deadline: February 16, 2020, 23:59:59 AoE (Anywhere on Earth)
Notification to Authors: April 6, 2020
Final Paper Submission Deadline: April 27, 2020
Conference: June 24-26, 2020

General Information

The annual DIMVA conference serves as a premier forum for advancing the state of the art in the broader areas of intrusion detection, malware analysis, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas. DIMVA is organized by the special interest group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI). The conference proceedings will appear in Springer Lecture Notes in Computer Science (LNCS) series.

Types of Solicited Submissions:

DIMVA solicits submissions of high-quality, original scientific papers presenting novel research on malware analysis, intrusion detection, vulnerability assessment, and related systems security topics. We invite submissions of two types:

FULL PAPERS, presenting novel and mature research results. Full papers are limited to 20 pages in Springer LNCS format, including bibliography and appendices.

SHORT PAPERS, presenting original, still ongoing work that has not yet reached the maturity required for a full paper. Short papers are limited to 10 pages in LNCS format, including bibliography and appendices. Short papers will be included in the proceedings. The title of short papers **must start** with the words “Extended Abstract”.

Papers that do not follow the above formatting guidelines may be rejected without review.

Indicative topics of interest include (but are not limited to):

Intrusions

- Novel approaches and domains
- Insider detection
- Prevention and response
- Data leakage, exfiltration, and poisoning
- Result correlation and cooperation
- Evasion and other attacks
- Potentials and limitations
- Operational experiences
- Privacy, legal, and social aspects
- Targeted attacks

Malware

- Automated analyses
- Behavioral models
- Prevention and containment
- Classification
- Lineage
- Forensics and recovery
- Underground economy
- Vulnerabilities in malware

Vulnerability detection

- Vulnerability prevention
- Vulnerability analysis
- Exploitation and defenses
- Hardware vulnerabilities
- Situational awareness
- Active probing

Papers will be judged on novelty, significance, correctness, and clarity. We expect all papers to provide enough detail to enable reproducibility of the experimental results. We encourage papers that bridge research in different communities. We also welcome experience papers that clearly articulate lessons learnt.

Submission Guidelines:

DIMVA 2020 adopts a double-blind reviewing process. All submissions should be appropriately anonymized. Author names and affiliations must be excluded from the paper. Furthermore, authors should avoid obvious self-references, and should cite their own previous work in third person, whenever necessary. Papers that are not properly anonymized risk being rejected without review.

Submissions must be original work and may not be under submission to another venue at the time of review. At least one author of each accepted paper is required to physically present the submitted work at the conference, for the paper to be included in the proceedings.

Authors are encouraged to submit code appropriately anonymized, using, e.g., https://anonymous.4open.science/

Papers can be submitted using the following submission website: https://dimva2020.hotcrp.com

Ethical Considerations:

Submissions that report experiments with data gathered from human subjects should disclose whether the research received approval from an institutional ethics review board (IRB), if applicable, and what measures were adopted to minimize risks to privacy.

Submissions that describe experiments related to vulnerabilities in software or systems should discuss the steps taken to avoid negatively affecting any third-parties (e.g., in the case of probing of network devices), and how the authors plan to responsibly disclose the vulnerabilities to the appropriate software or system vendors or owners before publication.

If you have any questions, please contact the program chairs at pc-chairs@dimva.org

Organizing Committee:

General Chair
Nuno Neves, University of Lisboa, Portugal

Program Chair
Clémentine Maurice, CNRS, IRISA, France

Program Co-Chair
Leyla Bilge, Symantec Research Labs, France

Publications Chair
Gianluca Stringhini, Boston University, USA

Publicity Chair
Pedro Ferreira, University of Lisboa, Portugal

Sponsor Chair
Thomas Schreck, Munich University of Applied Sciences, Germany

Local Arrangements Chair
Ibéria Medeiros, University of Lisboa, Portugal

Program Committee:

Magnus Almgren, Chalmers University of Technology, Sweden
Elias Athanasopoulos, University of Cyprus, Cyprus
Davide Balzarotti, Eurecom, France
Sébastien Bardin, CEA LIST, France
Gregory Blanc, Télécom SudParis, Institut Polytechnique de Paris, France
Herbert Bos, Vrije Universiteit Amsterdam, Netherlands
Juan Caballero, IMDEA Software Institute, Spain
Lucas Davi, University of Duisburg-Essen, Germany
Sven Dietrich, City University of New York, USA
Ulrich Flegel, Infineon Technologies AG, Germany
Aurélien Francillon, Eurecom, France
Yanick Fratantonio, Eurecom, France
Mariano Graziano, Cisco Talos, France
Daniel Gruss, Graz University of Technology, Austria
Christophe Hauser, University of Southern California, USA
Alexandros Kapravelos, North Carolina State University, USA
Vasileios Kemerlis, Brown University, USA
Christian Kreibich, Corelight, USA
Anil Kurmus, IBM Research - Zurich, Switzerland
Pierre Laperdrix, CNRS, Univ. Lille, France
Pavel Laskov, University of Liechtenstein, Liechtenstein
Martina Lindorfer, TU Wien, Austria
Michael Meier, University of Bonn and Fraunhofer FKIE, Germany
Marius Muench, Vrije Universiteit Amsterdam, Netherlands
Nick Nikiforakis, Stony Brook University, USA
Yossi Oren, BGU, Israel
Giancarlo Pelegrino, CISPA Helmholtz Center for Information Security, Germany

Fabio Pierazzi, King's College London, UK
Michalis Polychronakis, Stony Brook University, USA
Georgios Portokalidis, Stevens Institute of Technology, USA
Thomas Schreck, Munich University of Applied Sciences, Germany
Michael Schwarz, Graz University of Technology, Austria
Deborah Shands, SRI International, USA
Seungwon Shin, KAIST, South Korea
Yan Shoshitaishvili, Arizona State University, USA
Asia Slowinska, IBM, Netherlands
Gianluca Stringhini, Boston University, USA
Juan Tapiador, Universidad Carlos III, Spain
Sam Thomas, CentraleSupélec, France
Erik van der Kouwe, Vrije Universiteit Amsterdam, Netherlands
Mathy Vanhoef, New York University Abu Dhabi, UAE
Pierre-Antoine Vervier, Symantec Research Labs, France

Steering Committee:

Chairs
Ulrich Flegel, Infineon Technologies, Germany
Michael Meier, University of Bonn and Fraunhofer FKIE, Germany

Members
Magnus Almgren, Chalmers University of Technology, Sweden
Sébastien Bardin, CEA, France
Gregory Blanc, Télécom SudParis, France
Herbert Bos, Vrije Universiteit Amsterdam, Netherlands
Danilo M. Bruschi, Università degli Studi di Milano, Italy
Roland Bueschkes, RWE AG, Germany
Juan Caballero, IMDEA Software Institute, Spain
Lorenzo Cavallaro, King’s College London, UK
Hervé Debar, Télécom SudParis, France
Sven Dietrich, City University of New York, USA
Cristiano Giuffrida, Vrije Universiteit Amsterdam, Netherlands
Bernhard Haemmerli, Acris GmbH and HSLU Lucerne, Switzerland
Thorsten Holz, Ruhr-University Bochum, Germany
Marko Jahnke, CSIRT, German Federal Authority, Germany
Klaus Julisch, Deloitte, Switzerland
Christian Kreibich, ICSI, USA
Christopher Kruegel, UC Santa Barbara, USA
Pavel Laskov, University of Liechtenstein, Liechtenstein
Federico Maggi, Trend Micro Research, Italy

Roberto Perdisci, University of Georgia and Georgia Institute of Technology, USA
Michalis Polychronakis, Stony Brook University, USA
Konrad Rieck, TU Braunschweig, Germany
Jean-Pierre Seifert, Technical University Berlin, Germany
Robin Sommer, ICSI/LBNL, USA
Urko Zurutuza, Mondragon University, Spain

Sponsorship Opportunities:

We solicit interested organizations to serve as sponsors for DIMVA 2020. Please contact the sponsor chair (sponsor-chair@dimva.org) for details regarding sponsorship.